LARA LICENSING AND REGULATORY AFFAIRS CUSTOMER DRIVEN. BUSINESS MINDED.	**Effective Date:**	09-12-2011
	Policy #:	G-20
	Supersedes:	
Subject: **Information Privacy and Security Handling**	**Page:**	1 of 3

PURPOSE

The department's Information Privacy and Security Policy require controls to manage risks to the confidentiality, integrity, and availability of department information. These information handling standards define the controls required for sensitive department information in any form. These controls represent a minimum standard to protect sensitive department information. Additional controls required by applicable laws, regulations, or standards governing specific forms of data may also apply.

Each individual who creates, uses, processes, stores, transfers, administers, or destroys sensitive department information must comply with this standard. In addition, all computers owned by the state or connected to the state network are subject to applicable Department of Technology, Management and Budget (DTMB) standards.

Creation

Department employees create records as part of conducting business. These records document the decisions and activities of our operations. The appropriate creation and maintenance throughout their entire life cycle is essential. Sensitive information in department records is an area of critical concern because of the severe risks to the department and individuals should records be mishandled or information inappropriately accessed or disclosed. Accordingly, records containing sensitive information should exist only in areas where there is a legitimate and justifiable business need, as authorized by the Information Privacy Officer (IPO), and maintained under controls outlined in this document. Work areas should identify and track department records through their life cycle using records retention schedules. A first priority should be identifying sensitive information. Records schedules (1) document the existence of these materials and the rationale to keep them and (2) help ensure their availability while they are vital as administrative or historical records. Retention schedules also ensure the timely disposal of inactive records, thereby mitigating the risk of exposure of information that no longer serves an active administrative or historical function.

Bureaus shall review the data they are assigned responsibility for and classify any sensitive information that will require elevated handling standards. Bureaus may also identify restricted information and establish appropriate handling standards in consideration of their privileged or confidential nature.

Access

Information designated to be sensitive requires strict control and very limited access and disclosure; it may also be subject to legal restrictions. Only department employees and agents with a signed confidentiality agreement on file may access sensitive information. Any other disclosure of sensitive information requires the written approval of the appropriate bureau director, in consultation with the Information Privacy Officer.

Use, Transmission, and Storage

The following controls are **required** when using, transmitting, or storing sensitive information.

- Avoid displaying or discussing it in an environment where it may be viewed or overheard by unauthorized individuals.
- Do not leave keys or other access tools for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.
- When printing, photocopying, or faxing, ensure that only authorized personnel will be able to see the output.
- Store paper documents in a locked drawer, a locked room, or another secure location approved by the bureau director.
- Properly identify such information as sensitive to all recipients, by labeling it "Sensitive," providing training to personnel, explicitly mentioning the classification, or similar means.
- Encrypt electronic information using an encryption algorithm approved by DTMB when:
    - Placing it on removable media.
    - Placing it on mobile computers (e.g., laptops, PDAs, smart phones).
    - Sending it via e-mail to non-michigan.gov addresses.
    - Sending it via file transfer protocol (FTP) outside the State's network.
- Do not send this information via instant message or unsecured file transfer unless encrypted.
- Follow an established and documented software development lifecycle when building applications that process sensitive information.

Transport

The following controls are required when transporting sensitive information:

- When sending such information by mail (including U.S. Postal Service, UPS, FedEx, etc.) in non-electronic form, the sender must obtain tracking and signature confirmation services and use a tamper-evident sealed package.
- Do not send unencrypted sensitive information by interoffice mail.
- When carrying unencrypted sensitive information, or devices containing such information, ensure that it is physically secure at all times.
- Restricted information cannot be disseminated without following approved procedures, including proper supervisory approval. Sensitive information cannot be removed from an approved secure location without prior approval of the Data Steward.

Destruction

- Department records should be destroyed only in accordance with the General Retention Schedules for State Government and any other retention policies approved in writing by the Information Privacy Officer.
- Destroy electronic records of department information using DTMB approved method as described in DTMB Procedure 1350.90. Reformatting a hard drive is not sufficient to securely remove all data.
- Crosscut shred or use a secured shredding system to destroy all sensitive information in paper form, including all transitory work products (e.g., unused copies, drafts, notes).

ENFORCEMENT

All department staff must report suspected violations of this policy to the Information Privacy Officer. Violations of this policy, including the failure to report one's own improper transmission of sensitive data, are grounds for discipline, up to and including dismissal.